CLAIMS

1. A system for end user control of the distribution and maintenance of end user personal profile data in a data communications system providing communication between applications comprising and/or communicating with service/information/content providers or holding means (DB) holding end user personal profile data,

c h a r a c t e r i z e d i n

that it comprises a personal profile protection network with at least one central protection server means, comprising or communicating with information holding means holding personal protection profile information, and a number of distributed access means, e.g. software modules, whereby for each of said applications at least one access means is provided, and in that grant/reject of an access request for/to end user personal profile data by a requesting application is determined by the central protection server in communication with a requesting application and/or an information providing application, in that translating means are provided for identity translation and that the identity of a requesting application will be concealed for an information providing application, and vice versa.

2. A system according to claim 1,

c h a r a c t e r i z e d i n

that there is one access means for each application.

3. A system according to claim 1 or 2,

c h a r a c t e r i z e d i n

that there are a plurality, e.g. a cluster, of access means for at least one application.

4. A system according to claim 1, 2 or 3,
c h a r a c t e r i z e d i n
that the central server means only comprises personal protection profile data, the personal profile data being distributed throughout the system.

5. A system according to claim 4,
c h a r a c t e r i z e d i n
that the personal protection profile data comprises information about, for each end user of the system, which of the end user personal profile data that should be accessible by which application(s).

6. A system according to claim 4,
c h a r a c t e r i z e d i n
that the personal protection profiles are assigned one of a given number of security levels, the lowest level e.g. indicating that for all personal profile data access is prevented for every application, the highest e.g. indicating that all personal profile data is freely available.

7. A system according to any one of the preceding claims,
c h a r a c t e r i z e d i n
that the interface between an application and the respective access means comprises an Application Programmable Interface (API) based on (using) a generic markup language.

8. A system according to claim 7,
c h a r a c t e r i z e d i n
that the generic markup language is XML.

9. A system according to claim 7 or 8,

characterized in
that access to requested end user personal profile data is granted/rejected by the central server in communication with the requesting application.

10. A system according to claim 7 or 8,
characterized in
that access to requested end user personal profile data is granted/rejected by the central server in communication with the information providing application.

11. A system according to claim 7 or 8,
characterized in
that access to requested end user personal profile data is granted/rejected by the central server in communication with the requesting application and the information providing application.

12. A system according to claim 9, 10 or 11,
characterized in
that first user identity translating means (e.g. encrypting means) are provided at least in the central server means.

13. A system according to claim 10, 11 or 12,
characterized in
that second user identity translating means are provided in the access means of the requesting application.

14. A system according to any one of claims 7-13,
characterized in
that for each pair of applications of the system a general DTD (Document Type Definition) is given to define allowed flow of personal data.

15. A system according to claim 14,
c h a r a c t e r i z e d i n
that for each user a specific user unique DTD agreement is given.

16. A system according to any one claims 7-15,
c h a r a c t e r i z e d i n
that an access request for end user profile data is transported from the requesting application to its access means e.g. using RMI, and in that the access request includes a user identity associated with the requested personal end user profile.

17. A system according to claim 16,
c h a r a c t e r i z e d i n
that the request is transported as an XML transport object (XML Node tree container) tagged with information about the requested end user personal profile data.

18. A system according to claim 16 or 17,
c h a r a c t e r i z e d i n
that the HTTPS protocol is used for communication between the access means of the requesting/information holding application and the central server means.

19. A system according to any one of the preceding claims,
c h a r a c t e r i z e d i n
that the access means of the information requesting and/or providing application(s) comprise(s) means for encrypting the user identity associated with the requested end user profile.

20. A system according to any one of the preceding claims,
c h a r a c t e r i z e d i n

that the request is digitally signed with a private key of the access means of the requesting application and/or with a private key of the access means of the information providing application.

21. A system according to claim 20,
c h a r a c t e r i z e d i n
that the request is digitally signed with a private key of the central server means, and in that the digital signature(s) of the access means are verified in the central server means.

22. A system according to claim 21,
c h a r a c t e r i z e d i n
that the central server means comprises means for encrypting at least the user identity associated with the requested information used by the information providing information.

23. A system according to any one of the preceding claims,
c h a r a c t e r i z e d i n
that at least some of the applications comprise a cache memory respectively for temporarily holding information about access requests, such that a previously used session can be reused, at least for a given time period.

24. A personal profile (privacy) control network for controlling the access to personal profile data,
c h a r a c t e r i z e d i n
that it comprises at least one central protection server means, comprising or communicating with information holding means holding personal protection profile information, and a number of distributed access means, e.g. software modules, at least one access means respectively interfacing each of a number of applications, the central protection server means comprising means for translating and verifying identities, and in that a request

for access to personal profile data by a requesting application is communicated to the requesting application access means and granted/rejected by the central server means in communication with the access means of the requesting application and/or the information providing application, and in that the user identity used by the requesting application is concealed for the information providing application and vice versa.

25. A personal profile control network according to claim 24, c h a r a c t e r i z e d i n that the interface between an application and the respective access means is based on a generic mark-up language.

26. A personal profile control network according to claim 25, c h a r a c t e r i z e d i n that the generic mark-up language is XML.

27. A personal profile control network according to any one of claims 24-26, c h a r a c t e r i z e d i n that the information holding means of the central server means comprises, for each user of the system, a personal protection profile, and in that the personal protection profiles are end user controlled.

28. A personal profile control network according to claim 27, c h a r a c t e r i z e d i n that the central server means and at least one of the information requesting/providing access means digitally sign a request for personal profile data with the respective private key, and in that the digital signatures are verified by the central server means.

29. A method of controlling access to personal data within a personal end user profile in a data communication network running

a number of applications comprising or communicating with information holding means,
c h a r a c t e r i z e d i n
that it comprises the steps of:

- providing an access request from a requesting application to an access means associated with the requesting application using a generic mark-up language, e.g. XML,
- forwarding the request from the access means to a central server means with information holding means holding personal protection profiles for the end users in the system;
- performing user identification encryption, such that the user identification of the requesting application will be concealed from an information providing application, and vice versa;
- establishing, by using the request and the personal protection profile whether access is to be granted or denied;
  if access to the requested personal profile is to be granted,
- confirming to the access means of the requesting application whether access is to be granted or not, preferably after digitally signing the request;
- allowing transfer of the encrypted and preferably digitally signed request to the information providing application.

30. The method according to claim 29,
c h a r a c t e r i z e d i n
that the request of a requesting application relates to getting access to data/fetching data in a personal profile and in that, for a granted request, the method comprises the step of:

- transferring the requested data via the access means of an information providing application over a data communication network, e.g. Internet, to the access means of the requesting application.

31. The method according to claim 29,

c h a r a c t e r i z e d i n
that the request of a requesting application relates to setting/updating data in a personal profile, and in that, for a granted request the method further comprises the step of:
- transferring the data to be set/updated data to the information providing application over the data communication network.

32. A method of controlling access to personal data within a personal end user profile in a data communication network running a number of applications comprising, or communicating, with information holding means,
c h a r a c t e r i z e d i n
that it comprises the steps of:
- forwarding a request for access to data within a personal profile from a requesting application via at least one distributed access means to a central server means;
- establishing in the central server means whether access to requested data should be allowed or not by comparing the request with an end user controlled personal protection profile;
- providing the at least one distributed access means with information as to whether access is allowable or not, such that if access is allowable, the data communication network can be used for giving the requesting application access to the requested data without the identity of the requesting application being visible to the application able to provide access to the requested data, and vice versa.

33. A method according to claim 32,
c h a r a c t e r i z e d i n
that it further comprises the steps of:

- encrypting a user identity associated with the requested end user profile into the request at the central server means or at access means associated with the requesting application;
- decrypting the user identity at access means associated with the information providing application.

34. The method according to claim 32 or 33,
c h a r a c t e r i z e d i n
that it comprises the steps of:
- digitally signing the request at one or more of the access means associated with the information requesting application, the access means associated with the information providing application and the central server means, said access means and the central server means constituting a personal profile data protection network.